Appl. No. 10/643,564
Amendment and Response dated May 3, 2007
Reply to Office Action of March 15, 2007

REMARKS

Claims 1 to 24 were pending in the application at the time of examination.

The specification is amended to correct a minor typographical error.

Claims 2 and 12-14 are cancelled without prejudice.

New Claims 25-28 are added.

Claims 1, 6, 7, 8, 10, 15 and 20 are amended.

Claim 1 is amended to incorporate the limitations of Claim 2 as explained in more detail herein with regard to the 35 U.S.C. 101 rejection. Consequently, Claims 7, 8 and 10, which originally depended from Claim 2, are amended to now depend from Claim 1 and provide proper dependency.

Claim 6 is amended to correct a grammatical informality as required by the Examiner.

Claims 15 and 20 are amended to provide antecedent agreement with the term "host computer system".

Applicants submit the amendments and new claims are supported in the application as filed, and that no new matter has been added.

Applicants respectfully request reconsideration of the application.

Claims 1, 3-11, and 15-28 are presented for examination.

Claim Objections

In the Office Action at page 2, the Examiner required correction of Claim 6 to recite "a destination port".

Applicants have amended Claim 6 to recite "a destination port". Applicants respectfully submit Claim 6 as amended overcomes the Examiner's objection. Applicants respectfully request reconsideration and withdrawal of the objection to Claim 6.

Appl. No. 10/643,564
Amendment and Response dated May 3, 2007
Reply to Office Action of March 15, 2007

Rejections under 35 U.S.C. 101

Claims 1 and 3-6

In the Office Action at page 2, the Examiner rejected Claims 1 and 3-6 under 35 U.S.C. 101 as directed to non-statutory subject matter and stated in part:

> ...In order to meet the "useful" requirement, there must be some application implemented based on the results. For example, claim 2 is not rejected under 35 U.S.C 101 since the tangible/useful result is the step of "providing a notification of the malicious code detection" once the malicious code is detected.

Applicants have amended Claim 1 to incorporate the limitations of Claim 2. Accordingly, Applicants respectfully submit Claim 1 as amended recites statutory subject matter and overcomes the Examiner's rejection under 35 U.S.C. 101. Claims 3-6 depend from Claim 1 and so also recite statutory subject matter and overcome the Examiner's rejection.

Applicants respectfully request reconsideration and withdrawal of the 35 U.S.C. 101 rejections of each of Claims 1 and 3-6.

Claims 12-14

In the Office Action at pages 2-3, the Examiner rejected Claims 12-14 as directed to non-statutory subject matter.

Applicants have cancelled Claims 12-14 and so have rendered the 35 U.S.C. 101 rejections of each of Claims 12-14 moot.

Rejections under 35 U.S.C. 112

In the Office Action at page 3, the Examiner rejected Claims 12-14 under 35 U.S.C. 112, second paragraph. Applicants have cancelled Claims 12-14 and so have rendered the 35 U.S.C. 112 rejections of each of Claims 12-14 moot.

Appl. No. 10/643,564
Amendment and Response dated May 3, 2007
Reply to Office Action of March 15, 2007

Rejections under 35 U.S.C. 102(b)

In the Office Action at page 3, the Examiner rejected Claims 1-7 and 12-14 under 35 U.S.C. 102(b) as being fully anticipated by Hockey, WO 02/19069 A2, hereinafter Hockey.

<u>Claims 1 and 2-7 are not anticipated by and are patentable over Hockey</u>

Claim 1

Applicants respectfully traverse the anticipation rejection of each of Claims 1 and 3-7; Claim 2 was cancelled as earlier remarked.

With regard to independent Claim 1, in the Office Action at page 3, the Examiner states:

> "Hockey teaches a method comprising: comparing outbound traffic on a host computer system to inbound traffic on the host computer system (pg. 19, line 10-pg. 20, line 3)….

Applicants respectfully submit that the citation to Hockey relied on by the Examiner does not teach or suggest comparing outbound traffic on a host computer system to inbound traffic on the host computer system.

The citation to Hockey at page 19, lines 10-25 describes in part:

> The generated digest (or digests) is stored in a memory, together with the internet protocol (IP) address of where the message came from, sender information and destination details, and a timestamp to serve as a record of when the message was received….
> …To determine whether the textual content of the message or the attached files match those from previous messages received by the mail server 100, **the digest is compared with existing digests stored in memory** in step 304 and any matches noted in step 310. (emphasis added)

Appl. No. 10/643,564
Amendment and Response dated May 3, 2007
Reply to Office Action of March 15, 2007

With regard to the "messages", Hockey at page 17, lines 1-10 describes in part:

> Preferably, the software is loaded permanently on a mail server, and remains in a quiescent state until an email message arrives at the server, typically from another server via SMTP. In step 300, **the software intercepts <u>an incoming mail message</u> and reads it into memory**….   (emphasis added)

With regard to the "digests", Hockey at page 17, line 33-page 18, line 17 describes in part:

> **A characteristic numerical representation is generated from the combined subject line 215 and message content**, in step 302….
> …Such a characteristic numerical representation, or "hash" as known to one of skill of the art, is a message digest algorithm which takes a message of arbitrary length and produces a numerical representation comprising a number of bits sufficiently small **to form a condensed digest of the original message** and allow fast and straight-forward searching, but sufficiently large to be essentially unique.   (emphasis added)

Based on the above, Applicants submit the references to Hockey relied on by the Examiner at most describe comparison of **inbound emails to inbound emails, i.e., comparison of inbound traffic to inbound traffic.**

Distinguishably, Applicants' Claim 1 recites in part at least:

> …comparing **outbound traffic** on a host computer system to **inbound traffic** on the host computer system… (emphasis added)

Inbound traffic is distinguishable from outbound traffic (see for example Applicants' specification at page 6, lines 2-22). Accordingly, Applicants submit the reference to Hockey relied on by the Examiner does not teach at least the above

Appl. No. 10/643,564
Amendment and Response dated May 3, 2007
Reply to Office Action of March 15, 2007

element of Claim 1, and thus does not support an anticipation rejection of Claim 1.

Claims 3-11 depend from Claim 1, and thus for at least the same reasons as Claim 1, are not anticipated by and are patentable over Hockey.

Applicants respectfully request reconsideration and withdrawal of the 35 U.S.C. 102(b) anticipation rejection of each of Claims 1 and 3-7.

Claims 12-14

Claims 12-14 were cancelled without prejudice and so have rendered the 35 U.S.C. 102(b) rejections of each of Claims 12-14 moot.

Rejections under 35 U.S.C. 102(e)

In the Office Action at page 6, the Examiner rejected Claims 15-24 under 35 U.S.C. 102(e) as being fully anticipated by Chesla et al., US Pub. No. 2004/0250124, hereinafter Chesla.

Claim 15-24 are not anticipated by and are patentable over Chesla

Claim 15

Applicants respectfully traverse the anticipation rejections of each of Claims 15-19.

With regard to independent Claim 15, in the Office Action at page 3, the Examiner states in part:

> ...Chesla et al. teach a method comprising:
> ...comparing at least a portion of the copied inbound traffic with at least a portion of the copied outbound traffic (par. 137); determining if malicious code is detected on the host computer system based on the comparing (par. 137)....

.Appl.. No. 10/643,564
Amendment and Response dated May 3, 2007
Reply to Office Action of March 15, 2007

Applicants respectfully submit that the citation to Chesla relied on by the Examiner does not teach or suggest comparing at least a portion of the copied inbound traffic with at least a portion of the copied outbound traffic.

The citation to Chesla at par. 137 describes in part:

> On the other hand, if the network flood controller determined at step 112 that the filtering was effective, i.e., the degree of the attack decreased as a result of filtering, the controller reacts to this positive feedback by increasing the filtering period and continuing to monitor the attack, at an attack monitoring step 118. **In order to determine whether the attack is continuing, the controller directs FIS module 62 to evaluate both unfiltered traffic from WAN 26 and filtered traffic from filtering module 70. The level of attack in both of these streams is compared, at an attack stop check step 120.** If both streams are evaluated as not containing an attack, the controller directs the filtering module to discontinue filtering, at a stop filtering step 122, and the controller resumes statistics collection at step 100 and attack monitoring at step 101. On the other hand, if the attack continues, the controller checks whether the attack level has increased, at a attack level check step 124. A change in the attack level is interpreted either as an indication that the nature of the attack has changed, or as an indication that a second, independent attack has begun in addition to the attack already detected….

Applicants respectfully submit that the above citation to Chesla is excerpted from a description of FIG. 3 "…which is a flow chart that schematically illustrates, in overview, a method for detecting and filtering an attack on a protected network 22…" (Chesla, page 8, par. 130), and at most describes a comparison of filtered **incoming traffic** and unfiltered **incoming traffic**.

For example, with regard to the "unfiltered traffic from WAN 26", Chesla at page 8, par. 132 describes in part:

.Appl., No. 10/643,564
Amendment and Response dated May 3, 2007
Reply to Office Action of March 15, 2007

> Once the baseline parameters have been set,
> network flood protection module 50 **directs FIS module
> 62 to monitor traffic from WAN 26** in order to detect
> an attack, at an attack monitoring step 101.
> (emphasis added)

Thus, Applicants submit at most the "unfiltered traffic from WAN 26" monitored by FIS module 62 is **incoming traffic** from WAN 26. (See also Fig. 2 of Chesla showing flow of incoming traffic from WAN 26.)

With regard to the "filtered traffic from filtering module 70", Chesla at page 8, par. 135 describes in part:

> On the other hand, if the anomaly is not
> transient, **filtering module 70 filters incoming
> traffic,** at a filtering step 110, using the signatures
> determined by trapping module 68 at step 106.
> (emphasis added)

Thus, Applicants submit at most the "filtered traffic from filtering module 70" is again **incoming traffic** that has been filtered by filtering module 70.

Based on the above, Applicants submit at most the citation to Chesla relied on by the Examiner describes **comparison of unfiltered incoming traffic to filtered incoming traffic, i.e., comparison of incoming traffic to incoming traffic**.

Distinguishably, Applicants' Claim 15 recites in part at least:

> ...comparing at least a portion of the copied
> **inbound traffic** with at least a portion of the copied
> **outbound traffic...** (emphasis added)

As earlier remarked with the regard to the anticipation rejection of Claim 1, inbound traffic is distinguishable from outbound traffic. Accordingly, Applicants submit the reference to Chesla relied on by the Examiner does not teach at least the above element of Claim 15, and thus does not support an anticipation rejection of Claim 15.

.Appl., No. 10/643,564
Amendment and Response dated May 3, 2007
Reply to Office Action of March 15, 2007

Claims 16-19 depend from Claim 15, and thus for at least the same reasons as Claim 15, are not anticipated by and are patentable over Chesla.

Applicants respectfully request reconsideration and withdrawal of the 35 U.S.C. 102(e) anticipation rejection of each of Claims 15-19.

Claim 20

Applicants respectfully traverse the anticipation rejections of each of Claims 20-24.

Applicants' Claim 20 recites in part at least:

> comparing at least a portion of the copied **inbound traffic** with at least a portion of the buffered **outbound traffic**…(emphasis added)

Applicants respectfully submit that for at least the same reasons discussed with regard to the anticipation rejection of Claim 15, herein incorporated by reference, Claim 20 is not anticipated by and is patentable over Chesla.

Claims 21-24 depend from Claim 20, and thus for at least the same reasons as Claim 20, are not anticipated by and are patentable over Chesla.

Applicants respectfully request reconsideration and withdrawal of the 35 U.S.C. 102(e) anticipation rejection of each of Claims 20-24.

Rejections under 35 U.S.C. 103(a)

Claims 8-11 are not obvious in view of and are patentable over Hockey in view of Chesla

In the Office Action at page 9, the Examiner rejected Claims 8-11 under 35 U.S.C. 103(a) as being unpatentable over Hockey as applied to Claim 2 and further in view of Chesla.

.Appl. No. 10/643,564
Amendment and Response dated May 3, 2007
Reply to Office Action of March 15, 2007

Claims 8-11

Applicants respectfully traverse the obviousness rejections of each of Claims 8-11.

Claims 8-11 each depend directly or indirectly from independent Claim 1.

Applicants respectfully submit that for at least the reasons earlier presented with respect to the 102(b) rejection of Claim 1, the cited reference to Hockey fails to teach or suggest at least "...**comparing outbound traffic on a host computer system to inbound traffic** on the host computer system..." as recited in part in Applicants' Claim 1 (emphasis added). Further, for at least the reasons earlier presented with respect to the 102(e) rejection of Claim 15, the cited reference to Chesla fails to teach or suggest at least "...**comparing at least a portion of the copied inbound traffic with at least a portion of the copied outbound traffic**..." as recited in part in Applicants' Claim 15. Thus, even in combination Chesla fails to correct the deficiencies of Hockey, and thus does not support an obviousness rejection of Claim 1.

Indeed, the Examiner did not reject Claim 1 as obvious over Hockey in view of Chesla.

Accordingly, Applicants respectfully submit that as Claim 1 is not obvious in view of and is patentable over the combination of Hockey and Chesla, and as Claims 8-11 depend from Claim 1, for at least the same reasons Claim 1 is not obvious over Hockey in view of Chesla, Claims 8-11 are also not obvious over Hockey in view Chesla.

Applicants respectfully request reconsideration and withdrawal of the 35 U.S.C. 103(a) rejections of each of Claims 8-11.

New Claims 25-28

Applicants respectfully submit that for at least the reason earlier presented with regard to the anticipation rejections of

Appl., No. 10/643,564
Amendment and Response dated May 3, 2007
Reply to Office Action of March 15, 2007

Claims 1, 15 ,and 20 and the obviousness rejections of Claims 8-11, new Claims 25-28 are also patentable over the cited references to Hockey and Chesla.

Applicants respectfully request entrance and allowance of Claims 25-28.

Conclusion

Claims 1 and 3-28 remain in the application. For the foregoing reasons, Applicants respectfully request allowance of all pending claims. If the Examiner has any questions relating to the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicant(s).

Request for Examiner Interview

Should the Examiner be of the opinion that this amendment does not place the Application in a condition for allowance, Applicants respectfully request an Examiner interview prior to issuance of the next communication from the USPTO to expedite prosecution.

Respectfully submitted,

Lisa A. Norris
Attorney for Applicant(s)
Reg. No. 44,976
Tel.: (831) 655-0880